EBA/GL/2019/02

25 februari 2019

Riktlinjer för utkontraktering

1. Efterlevnad och rapporteringsskyldigheter

Riktlinjernas status

1. Detta dokument innehåller riktlinjer som har utfärdats enligt artikel 16 i förordning (EU) nr 1093/2010[1]. I enlighet med artikel 16.3 i förordning (EU) nr 1093/2010 måste de behöriga myndigheterna och finansinstituten med alla tillgängliga medel söka följa riktlinjerna.

2. Av riktlinjerna framgår EBA:s syn på lämplig tillsynspraxis inom det europeiska systemet för finansiell tillsyn eller på hur unionslagstiftningen bör tillämpas inom ett särskilt område. Behöriga myndigheter enligt definitionen i artikel 4.2 i förordning (EU) nr 1093/2010 som berörs av riktlinjerna bör efterleva dem genom att på lämpligt sätt införliva dem i sin praxis (till exempel genom att ändra sitt rättsliga ramverk eller sina tillsynsrutiner), även när riktlinjerna i första hand riktas till institut och betalningsinstitut.

Rapporteringskrav

3. Enligt artikel 16.3 i förordning (EU) nr 1093/2010 måste de behöriga myndigheterna meddela EBA om att de följer eller avser att följa dessa riktlinjer, alternativt ange skälen till att de inte gör det, senast den [yyyy-mm-dd]. Om någon sådan anmälan inte inkommer inom denna tidsfrist kommer EBA att anse att de behöriga myndigheterna inte följer riktlinjerna. Anmälningar bör lämnas på det formulär som tillhandahålls på EBA:s webbplats till compliance@eba.europa.eu med referensen ”EBA/GL/2019/02”. Anmälningar bör inges av personer som har befogenhet att rapportera om hur reglerna efterlevs på de behöriga myndigheternas vägnar. Eventuella förändringar av efterlevnadsstatus måste också rapporteras till EBA.

4. Anmälningarna kommer att offentliggöras på EBA:s webbplats i enlighet med artikel 16.3.

[1] Europaparlamentets och rådets förordning (EU) nr 1093/2010 av den 24 november 2010 om inrättande av en europeisk tillsynsmyndighet (Europeiska bankmyndigheten), om ändring av beslut nr 716/2009/EG och om upphävande av kommissionens beslut 2009/78/EG (EUT L 331, 15.12.2010, s. 12).

2. Syfte, tillämpningsområde och definitioner

Syfte

5. Dessa riktlinjer preciserar de interna styrningsarrangemang, inklusive sund riskhantering, som institut, betalningsinstitut och institut för elektroniska pengar bör tillämpa vid utkontraktering av funktioner, särskilt avseende utkontrakteringen av kritiska eller viktiga funktioner.

6. Riktlinjerna preciserar hur de behöriga myndigheterna bör granska och övervaka arrangemangen som avses i föregående punkt utifrån artikel 97 i direktiv 2013/36/EU[2], översyns- och utvärderingsprocessen (ÖUP), artikel 9.3 i direktiv (EU) 2015/2366[3] och artikel 5.5 i direktiv 2009/110/EG[4] genom att fullgöra sin skyldighet att övervaka hur de enheter till vilka dessa riktlinjer riktar sig efterlever villkoren för sin auktorisation.

Mottagare

7. Dessa riktlinjer riktas till behöriga myndigheter som definieras artikel 4.1 led 40 i förordning (EU) nr 575/2013[5], inklusive Europeiska centralbanken avseende frågor som rör uppgifter som den tilldelats enligt förordning (EU) nr 1024/2013[6], till institut som definieras i artikel 4.1 led 3 i förordning (EU) nr 575/2013, till betalningsinstitut som definieras i artikel 4.4 i direktiv (EU) 2015/2366 och till institut för elektroniska pengar enligt den betydelse som anges i artikel 2.1 i direktiv 2009/110/EG. Leverantörer av kontoinformationstjänster som endast tillhandahåller tjänsten i punkt 8 i bilaga I i direktiv (EU) 2015/2366 omfattas inte av dessa riktlinjers tillämpningsområde, i enlighet med artikel 33 i det direktivet.

8. När det gäller dessa riktlinjer omfattar alla hänvisningar till ”betalningsinstitut” ”institut för elektroniska pengar” och alla hänvisningar till ”betalningstjänster” omfattar ”utfärdande av elektroniska pengar”.

---

[2] Europaparlamentets och rådets direktiv 2013/36/EU av den 26 juni 2013 om behörighet att utöva verksamhet i kreditinstitut och om tillsyn av kreditinstitut och värdepappersföretag, om ändring av direktiv 2002/87/EG och om upphävande av direktiv 2006/48/EG och 2006/49/EG.

[3] Europaparlamentets och rådets direktiv (EU) 2015/2366 av den 25 november 2015 om betaltjänster på den inre marknaden, om ändring av direktiven 2002/65/EG, 2009/110/EG och 2013/36/EU samt förordning (EU) nr 1093/2010 och om upphävande av direktiv 2007/64/EG.

[4] Europaparlamentets och rådets direktiv 2009/110/EG av den 16 september 2009 om rätten att starta och driva affärsverksamhet i institut för elektroniska pengar samt om tillsyn av sådan verksamhet, om ändring av direktiven 2005/60/EG och 2006/48/EG och om upphävande av direktiv 2000/46/EG.

[5] Europaparlamentets och rådets förordning (EU) nr 575/2013 av den 26 juni 2013 om tillsynskrav för kreditinstitut och värdepappersföretag och om ändring av förordning (EU) nr 648/2012 (EUT L 176, 27.6.2013, s. 1).

[6] Rådets förordning (EU) nr 1024/2013 av den 15 oktober 2013 om tilldelning av särskilda uppgifter till Europeiska centralbanken i fråga om politiken för tillsyn över kreditinstitut.

Tillämpningsområde

9. Utan att det påverkar direktiv 2014/65/EU [7] och kommissionens delegerade förordning (EU)2017/565 [8] (som innehåller villkor för utkontraktering för institut som tillhandahåller investeringstjänster och bedriver investeringsverksamhet, liksom relevanta riktlinjer utfärdade av Europeiska värdepappers- och marknadsmyndigheten om investeringstjänster och investeringsverksamhet) bör institut som definieras i artikel 3.1 led 3 i direktiv 2013/36/EU följa dessa riktlinjer på individuell nivå, undergruppsnivå och gruppnivå. De behöriga myndigheterna kan göra undantag från tillämpningen på individuell nivå enligt artikel 21 i direktiv 2013/36/EU eller artikel 109.1 i direktiv 2013/36/EU jämförd med artikel 7 i förordning (EU) nr 575/2013. Institut som är föremål för direktiv 2013/36/EU bör följa detta direktiv och dessa riktlinjer på gruppnivå och undergruppsnivå i enlighet med artikel 21 och artiklarna 108–110 i direktiv 2013/36/EU.

10. Utan att det påverkar artikel 8.3 i direktiv (EU) 2015/2366 och artikel 5.7 i direktiv 2009/110/EG bör betalningsinstitut och institut för elektroniska pengar följa dessa riktlinjer på individuell nivå.

11. Behöriga myndigheter som ansvarar för översynen av institut, betalningsinstitut och institut för elektroniska pengar bör följa dessa riktlinjer.

Definitioner

12. Om inget annat anges har begrepp som används och definieras i direktiv 2013/36/EU, förordning (EU) nr 575/2013, direktiv 2009/110/EG, direktiv (EU) 2015/2366 och EBA:s riktlinjer för intern styrning[9] samma betydelse i dessa riktlinjer. Dessutom gäller följande definitioner för dessa riktlinjer:

Utkontraktering	innebär ett arrangemang, oavsett form, mellan ett institut, betalningsinstitut eller institut för elektroniska pengar och en tjänsteleverantör där denna tjänsteleverantör utför en process, en tjänst eller en verksamhet som annars skulle ha utförts av institutet, betalningsinstitutet eller institutet för elektroniska pengar självt.
Funktion	innebär alla processer, tjänster eller verksamheter.

[7] Europaparlamentets och rådets direktiv 2014/65/EU av den 15 maj 2014 om marknader för finansiella instrument och om ändring av direktiv 2002/92/EG och av direktiv 2011/61/EU (EUT L 173, 12.6.2014, s. 349).

[8] Kommissionens delegerade förordning (EU) 2017/565 av den 25 april 2016 om komplettering av Europaparlamentets och rådets direktiv 2014/65/EU vad gäller organisatoriska krav och villkor för verksamheten i värdepappersföretag, och definitioner för tillämpning av direktivet (EUT L 87, 31.3.2017, s. 1).

[9] https://eba.europa.eu/regulation-and-policy/internal-governance/guidelines-on-internal-governance-revised-

Kritisk eller viktig funktion[10]	innefattar alla funktioner som anses vara kritiska eller viktiga enligt avsnitt 4 i dessa riktlinjer.
Underentreprenad	innebär en situation där en tjänsteleverantör enligt ett arrangemang för utkontraktering överför en utkontrakterad funktion vidare till en annan tjänsteleverantör.[11]
Tjänsteleverantör	innebär en tredje part som tar på sig en utkontrakterad process, tjänst eller verksamhet, eller delar därav, enligt ett arrangemang för utkontraktering.
Molntjänster	tjänster som tillhandahålls med hjälp av molnbaserade datortjänster, dvs. en modell som möjliggör en överallt förekommande och bekväm nätverkstillgång till ett antal delade konfigurerbara datorresurser (t.ex. nätverk, servrar, lagring, applikationer och tjänster) som snabbt kan tillhandahållas och levereras med minsta möjliga administration eller kontakt med tjänsteleverantören.
Offentligt moln	innebär molninfrastruktur som är tillgänglig för öppen användning av allmänheten.
Privat moln	innebär molninfrastruktur som är tillgänglig för exklusiv användning av ett enda institut eller betalningsinstitut.
Gruppmoln	innebär molninfrastruktur som är tillgänglig för exklusiv användning av en särskild grupp av institut, inklusive flera institut i en enda grupp.
Hybridmoln	innebär molninfrastruktur som består av två eller fler separata molninfrastrukturer.
Ledningsorgan	innebär ett instituts eller betalningsinstituts organ som har utsetts i enlighet med nationell lagstiftning, har mandat att att fastställa institutets eller betalningsinstitutets strategi, mål och allmänna inriktning, och som kontrollerar och övervakar ledningens beslutsfattande samt inkluderar personerna som i praktiken leder institutets eller betalningsinstitutets verksamhet samt cheferna och personerna som ansvarar för betalningsinstitutets ledning.

[10] Ordvalet ”kritisk eller viktig funktion” är baserat på ordvalet som används enligt direktiv 2014/65/EU (Mifid II) och kommissionens delegerade förordning (EU) 2017/565 som kompletterar Mifid ll. Det används endast vid utkontraktering och har inget att göra med definitionen av ”kritiska funktioner” i ramen för återhämtning och resolution som definieras i artikel 2.1.35 i direktiv 2014/59/EU (direktivet om inrättande av en ram för återhämtning och resolution av kreditinstitut och värdepappersföretag).

[11] För bedömningen gäller föreskrifterna i avsnitt 3; underentreprenad har även kallats ”kedjeutkontraktering” i andra EBA-dokument.

3. Genomförande

Tillämpningsdatum

13. Bortsett från punkt 63 b gäller dessa riktlinjer från den 30 september 2019 för alla arrangemang för utkontraktering som ingås, granskas eller ändras på eller efter detta datum. Punkt 63 b gäller från den 31 december 2021.

14. Institut och betalningsinstitut bör därefter granska och ändra befintliga arrangemang för utkontraktering för att säkerställa att dessa efterlever dessa riktlinjer.

15. Om granskningen av arrangemang för utkontraktering av kritiska eller viktiga funktioner inte är färdiga till den 31 december 2021 bör instituten och betalningsinstituten informera sina behöriga myndigheter om detta, inklusive åtgärder som planeras för att fullgöra granskningen eller den möjliga exitstrategin.

Övergångsbestämmelser

16. Institut och betalningsinstitut bör färdigställa dokumentationen av alla existerande arrangemang för utkontraktering, förutom för arrangemang för utkontraktering med leverantörer av molntjänster, i linje med dessa riktlinjer efter det första förnyelsedatumet för varje befintligt arrangemang för utkontraktering, dock senast den 31 december 2021.

Upphävande

17. Europeiska banktillsynskommitténs (CEBS) riktlinjer om utkontraktering av den 14 december 2006 och EBA:s rekommendationer om utkontraktering till molntjänstleverantörer[12] upphävs med verkan den 30 september 2019.

[12] Rekommendationer om utkontraktering till molntjänstleverantörer (EBA/REC/2017/03).

4. Riktlinjer för utkontraktering

Kapitel I – Proportionalitet: grupptillämpning och institutionella skyddssystem

1 Proportionalitet

18. När institut, betalningsinstitut och behöriga myndigheter tillämpar eller övervakar efterlevnad av dessa riktlinjer, bör de beakta proportionalitetsprincipen. Syftet med proportionalitetsprincipen är att säkerställa att styrformer, däribland de som gäller utkontraktering, stämmer överens med institutets eller betalningsinstitutets individuella riskprofil, karaktär och affärsmodell och med hur omfattande och komplex dess verksamhet är, så att målen inom regleringskraven uppnås på ett ändamålsenligt sätt.

19. När instituten och betalningsinstituten tillämpar de krav som fastställs i dessa riktlinjer, bör de ta hänsyn till de utkontrakterade funktionernas komplexitet, de risker som uppkommer genom utkontrakteringslösningen, hur kritisk eller viktig den utkontrakterade funktionen är samt hur utkontrakteringen potentiellt kan inverka på kontinuiteten i verksamheten.

20. När instituten, betalningsinstituten [13] och de behöriga myndigheterna tillämpar proportionalitetsprincipen, bör de ta hänsyn till de kriterier som anges i kapitel I i EBA:s riktlinjer för intern styrning i enlighet med artikel 74.2 i direktiv 2013/36/EU.

2 Utkontraktering hos grupper och institut som är medlemmar i ett institutionellt skyddssystem

21. I enlighet med artikel 109.2 i direktiv 2013/36/EU bör dessa riktlinjer också gälla på gruppnivå eller undergruppsnivå, med hänsyn till vad som ingår i den konsoliderade situationen.[14] För detta ändamål bör moderföretagen i EU eller moderföretaget i en medlemsstat säkerställa att interna styrformer, processer och mekanismer i deras dotterföretag, däribland betalningsinstitut, är konsekventa, välintegrerade och tillräckliga för att dessa riktlinjer ska kunna tillämpas ändamålsenligt på alla relevanta nivåer.

[13] Betalningsinstituten bör också se EBA:s riktlinjer enligt det andra betaltjänstdirektivet (PSD2) om information som ska lämnas för auktorisering av betalningsinstitut och institut för elektroniska pengar och registrering av leverantörer av kontoinformationstjänster; dessa riktlinjer finns tillgängliga på EBA:s webbplats under följande länk: https://www.eba.europa.eu/regulation-and-policy/payment-services-and-electronic-money/guidelines-on-security-measures-for-operational-and-security-risks-under-the-psd2

[14] Se artikel 4.1 punkt 47 och 48 i förordning (EU) nr 575/2013 gällande konsolideringens omfattning.

22. Institut och betalningsinstitut, i enlighet med punkt 21, och institut som i egenskap av medlemmar i ett institutionellt skyddssystem använder centralt tillhandahållna styrformer bör efterleva följande:

    a. När dessa institut eller betalningsinstitut har utkontrakteringslösningar med tjänsteleverantörer inom gruppen eller det institutionella skyddssystemet[15], behåller dessa instituts eller betalningsinstituts ledningsorgan, även för dessa utkontrakteringslösningar, det fulla ansvaret för efterlevnad av alla regleringskrav och för att dessa riktlinjer tillämpas ändamålsenligt.

    b. När dessa institut eller betalningsinstitut utkontrakterar interna kontrollfunktioners operativa uppgifter till en tjänsteleverantör inom gruppen eller det institutionella skyddssystemet, ska instituten för övervakning och revision av utkontrakteringslösningarna säkerställa att dessa operativa uppgifter, även för dessa utkontrakteringslösningar, utförs ändamålsenligt, däribland genom att erhålla lämpliga rapporter.

23. Utöver punkt 22 bör institut och betalningsinstitut inom en grupp som inga undantag har beviljats för grundat på artikel 109 i direktiv 2013/36/EU och artikel 7 i förordning (EU) nr 575/2013, institut som är ett centralt organ eller som är permanent underställda ett centralt organ som inga undantag har beviljats för grundat på artikel 21 i direktiv 2013/36/EU, eller institut som är medlemmar i ett institutionellt skyddssystem, ta hänsyn till följande:

    a. När den operativa övervakningen av utkontrakteringen är centraliserad (t.ex. som en del i ett ramavtal för övervakning av utkontrakteringslösningar), bör instituten och betalningsinstituten säkerställa att både oberoende övervakning av tjänsteleverantören och lämplig tillsyn från varje institut eller betalningsinstitut är möjlig, åtminstone för utkontrakterade kritiska eller viktiga funktioner, däribland genom att det erhålls, som minst årligen och på begäran från den centraliserade övervakningsfunktionen, rapporter som innehåller som minst en sammanfattning av riskbedömningen och resultatövervakningen. Dessutom bör instituten och betalningsinstituten av den centraliserade övervakningsfunktionen få en sammanfattning av de relevanta revisionsrapporterna för kritisk eller viktig utkontraktering, och på begäran hela revisionsrapporten.

    b. Instituten och betalningsinstituten bör säkerställa att deras ledningsorgan blir vederbörligen informerade om relevanta planerade förändringar avseende tjänsteleverantörer som övervakas centralt och vilken potentiell inverkan dessa förändringar kan få på de tillhandahållna kritiska eller viktiga funktionerna, inklusive en sammanfattning av riskanalysen, däribland juridiska risker, efterlevnad av

[15] I enlighet med artikel 113.7 i kapitalkravsförordningen menas med ett institutionellt skyddssystem ett avtalsgrundat eller lagstadgat skyddssystem som skyddar de institut som är medlemmar i systemet och särskilt sörjer för deras likviditet och solvens för att vid behov undvika konkurs.

regleringskrav och påverkan på tjänstenivåerna, så att de ska kunna bedöma påverkan som följer av dessa förändringar.

c. När dessa institut och betalningsinstitut inom gruppen, institut som är underställda ett centralt organ eller institut som ingår i ett institutionellt skyddssystem är beroende av en central förhandsbedömning av utkontrakteringslösningar, som nämns i avsnitt 12, bör varje institut och betalningsinstitut motta en sammanfattning av bedömningen och säkerställa att det tar hänsyn till dess särskilda struktur och risker inom beslutsprocessen.

d. När registret över alla befintliga utkontrakteringslösningar, som nämns i avsnitt 11, upprättas och upprätthålls centralt inom en grupp eller ett institutionellt skyddssystem, bör behöriga myndigheter, alla institut och betalningsinstitut kunna erhålla sitt individuella register utan onödigt dröjsmål. Detta register bör innefatta alla utkontrakteringslösningar, däribland utkontrakteringslösningar med tjänsteleverantörer inom den gruppen eller det institutionella skyddssystemet.

e. När dessa institut och betalningsinstitut är beroende av en avvecklingsplan för en kritisk eller viktig funktion som har upprättats på gruppnivå, inom det institutionella skyddssystemet eller av det centrala organet, bör alla institut och betalningsinstitut motta en sammanfattning av planen och vara övertygade om att planen kan verkställas ändamålsenligt.

24. När undantag har beviljats i enlighet med artikel 21 i direktiv 2013/36/EU eller artikel 109.1 i direktiv 2013/36/EU i samband med artikel 7 i förordning (EU) nr 575/2013, bör villkoren i dessa riktlinjer tillämpas av moderföretaget i en medlemsstat för sig självt och sina dotterföretag eller av det centrala organet och dess anknutna enheter som en helhet.

25. Institut och betalningsinstitut som är dotterföretag till ett moderföretag i EU eller till ett moderföretag i en medlemsstat som inga undantag har beviljats för grundat på artikel 21 i direktiv 2013/36/EU eller artikel 109.1 i direktiv 2013/36/EU i samband med artikel 7 i förordning (EU) nr 575/2013, bör säkerställa att de efterlever dessa riktlinjer på individuell basis.

Kapitel II – Bedömning av utkontrakteringslösningar

3 Utkontraktering

26. Institut och betalningsinstitut bör fastställa om ett avtal med en tredje part omfattas av definitionen för utkontraktering. I denna bedömning bör hänsyn tas till om funktionen (eller en del av den) som utkontrakteras till en tjänsteleverantör utförs på återkommande eller fortlöpande basis av tjänsteleverantören och om funktionen (eller delen av den) normalt skulle finnas bland de funktioner som skulle eller realistiskt skulle kunna utföras av institut eller

betalningsinstitut, även om institutet eller betalningsinstitutet inte tidigare har utfört denna funktion självt.

27. När ett arrangemang med en tjänsteleverantör omfattar flera olika funktioner, bör instituten och betalningsinstituten beakta alla aspekter av lösningen i sin bedömning; om t.ex. den tjänst som tillhandahålls innefattar att tillhandahålla maskinvara för datalagring och säkerhetskopiering av uppgifter, bör båda de aspekterna beaktas tillsammans.

28. Som allmän princip bör instituten och betalningsinstituten inte se följande som utkontraktering:

    a. En funktion som juridiskt sett måste utföras av en tjänsteleverantör, t.ex. lagstadgad revision.

    b. Marknadsinformationstjänster (t.ex. tillhandahållande av uppgifter från Bloomberg, Moody's, Standard & Poor's, Fitch).

    c. Globala nätverksinfrastrukturer (t.ex. Visa, MasterCard).

    d. Clearing- och avvecklingssyättsstem mellan clearingorganisationer, centrala motparts- och avräkningsinstitut och deras medlemmar.

    e. Globala infrastrukturer för finansiella meddelanden som är underställda tillsyn av relevanta myndigheter.

    f. Korrespondentbanktjänster.

    g. Förvärv av tjänster som annars inte skulle utföras av institutet eller betalningsinstitutet (t.ex. råd från en arkitekt, tillhandahållande av rättsligt yttranden och representation inför domstol och administrativa organ, städning, trädgårdsskötsel och lokalvård i institutets eller betalningsinstitutets lokaler, sjukvårdstjänster, service av firmabilar, catering, försäljningsautomattjänster, kontorstjänster, resetjänster, posttjänster, receptionister, sekreterare och växeloperatörer), varor (t.ex. plastkort, kortläsare, kontorsmaterial, persondatorer, möbler) eller allmännyttiga tjänster (t.ex. elektricitet, gas, vatten, telefonlinje).

4 Avgörande eller viktiga funktioner

29. Institut och betalningsinstitut bör alltid se en funktion som avgörande eller viktig i följande situationer:[16]

    a. När ett fel eller en brist i dess utförande allvarligt skulle försämra

[16] Se även artikel 30 i kommissionens delegerade förordning (EU) 2017/565 av den 25 april 2016 om komplettering av Europaparlamentets och rådets direktiv 2014/65/EU vad gäller organisatoriska krav och villkor för verksamheten i värdepappersföretag, och definitioner för tillämpning av det direktivet.

i. deras fortsatta uppfyllande av villkoren för deras auktorisation eller deras andra skyldigheter enligt direktiv 2013/36/EU, förordning (EU) nr 575/2013, direktiv 2014/65/EU, direktiv (EU) 2015/2366 och direktiv 2009/110/EG samt deras lagstadgade skyldigheter,

ii. deras finansiella resultat, eller

iii. sundheten eller kontinuiteten i deras banktjänst- och betaltjänstverksamhet.

b. När interna kontrollfunktioners operativa uppgifter utkontrakteras, såvida det inte fastställs vid bedömningen att det inte skulle få någon negativ inverkan på den interna kontrollfunktionens ändamålsenlighet om den utkontrakterade funktionen inte tillhandahölls eller tillhandahölls otillräckligt.

c. När de avser att utkontraktera bankverksamheters eller betalningstjänsters funktioner i en omfattning som skulle kräva auktorisation[17] från en behörig myndighet, som nämns i avsnitt 12.1.

30. När det gäller institut bör särskild uppmärksamhet ägnas åt att bedöma om funktioner är kritiska eller viktiga om utkontrakteringen gäller funktioner som har att göra med kärnaffärsområden och kritiska funktioner såsom definieras i artikel 2.1.35 och 2.1.36 i direktiv 2014/59/EU[18] och som identifieras av institut enligt de kriterier som fastställs i artiklarna 6 och 7 i kommissionens delegerade förordning (EU) 2016/778.[19] Funktioner som är nödvändiga för att utföra verksamheter i kärnaffärsområden eller kritiska funktioner bör ses som avgörande eller viktiga funktioner i dessa riktlinjer, såvida det inte fastställs i institutets bedömning att det inte skulle ha någon negativ inverkan på kärnaffärsområdets eller den kritiska funktionens operativa kontinuitet om den utkontrakterade funktionen inte tillhandahölls eller tillhandahölls otillräckligt.

31. Vid bedömningen av om en utkontrakteringslösning gäller en funktion som är kritisk eller viktig, ska instituten och betalningsinstituten ta hänsyn till, tillsammans med resultatet av riskbedömningen som beskrivs i avsnitt 12.2, åtminstone följande faktorer:

a. Om utkontrakteringslösningen har direkt samband med tillhandahållandet av de bankverksamheter eller betalningstjänster[20] som de är auktoriserade för.

---

[17] Se de verksamheter som förtecknas i bilaga I till direktiv 2013/36/EU.

[18] Europaparlamentets och rådets direktiv 2014/59/EU av den 15 maj 2014 om inrättande av en ram för återhämtning och resolution av kreditinstitut och värdepappersföretag och om ändring av rådets direktiv 82/891/EEG och Europaparlamentets och rådets direktiv 2001/24/EG, 2002/47/EG, 2004/25/EG, 2005/56/EG, 2007/36/EG, 2011/35/EU, 2012/30/EU och 2013/36/EU samt Europaparlamentets och rådets förordningar (EU) nr 1093/2010 och (EU) nr 648/2012 (EUT L 173, 12.6.2014, s. 190).

[19] Kommissionens delegerade förordning (EU) 2016/778 av den 2 februari 2016 om komplettering av Europaparlamentets och rådets direktiv 2014/59/EU vad gäller de omständigheter och villkor under vilka betalning av extraordinära efterhandsbidrag får skjutas upp helt eller delvis, och om kriterierna för fastställande av aktiviteter, tjänster och transaktioner avseende kritiska funktioner och för fastställande av affärsområden och kringtjänster avseende kärnaffärsområden (EUT L 131, 20.5.2016, s. 41).

[20] Se de verksamheter som förtecknas i bilaga I till direktiv 2013/36/EU.

b. Hur varje eventuell störning i den utkontrakterade funktionen, eller misslyckande från tjänsteleverantören med att tillhandahålla tjänsten kontinuerligt på de överenskomna tjänstenivåerna, påverkar deras

   i. kort- och långsiktiga finansiella motståndskraft och fortlevnad, inbegripet i tillämpliga fall deras tillgångar, kapital, kostnader, finansiering, likviditet, vinster och förluster,

   ii. affärskontinuitet och operativa motståndskraft,

   iii. operativa risk, inbegripet vad gäller uppförande, informations- och kommunikationsteknik och juridiska risker,

   iv. ryktesrisker,

   v. i tillämpliga fall återhämtnings- och resolutionsplanering, möjlighet till resolution och operativa kontinuitet i en situation med tidigt ingripande, återhämtning eller resolution.

c. Hur utkontrakteringslösningen potentiellt påverkar deras möjlighet att

   i. identifiera, övervaka och hantera alla risker,

   ii. efterleva alla juridiska krav och regleringskrav,

   iii. utföra lämpliga revisioner med avseende på den utkontrakterade funktionen.

d. Den potentiella påverkan på de tjänster som tillhandahålls till deras kunder.

e. Alla utkontrakteringslösningar, institutets eller betalningsinstitutets ansamlade exponering för samma tjänsteleverantör och den potentiella kumulativa påverkan av utkontrakteringslösningar i samma affärsområde.

f. Storleken och komplexiteten hos varje affärsområde som berörs.

g. Möjligheten att den föreslagna utkontrakteringslösningen skulle kunna utökas utan att ersätta eller ändra det underliggande avtalet.

h. Möjligheten att överföra den föreslagna utkontrakteringslösningen till en annan tjänsteleverantör, om det är nödvändigt eller önskvärt, både kontraktsmässigt och i praktiken, inklusive de uppskattade riskerna, försämringarna av affärskontinuiteten, kostnader och tidsramar för att göra detta (”utbytbarhet”).

i. Möjligheten att återintegrera den utkontrakterade funktionen i institutet eller betalningsinstitutet, om det är nödvändigt eller önskvärt.

j. Skydd av uppgifter och hur ett sekretessbrott eller misslyckande med att säkerställa tillgång till uppgifter och dataintegritet potentiellt skulle påverka institutet eller betalningsinstitutet och dess kunder, däribland sett till efterlevnaden av förordning (EU) 2016/679[21].

[21] Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning).

Kapitel III – Ramverk för styrning

5 Sunda styrformer och risker förknippade med tredje parter

32. Som del av den övergripande ramverket för intern kontroll [22], inklusive interna kontrollmekanismer [23], bör institut och betalningsinstitut ha ett heltäckande ramverk för riskhantering för hela institutet, som sträcker sig över alla affärsområden och interna enheter. Under denna ram bör instituten och betalningsinstituten identifiera och hantera alla risker, inbegripet risker som orsakas av arrangemang med tredje parter. Ramverket för riskhantering bör också göra det möjligt för instituten och betalningsinstituten att fatta välinformerade beslut om risktagande och säkerställa att riskhanteringsåtgärder genomförs på lämpligt sätt, även när det gäller it-risker.[24]

33. Med hänsyn till proportionalitetsprincipen i enlighet med avsnitt 1 bör instituten och betalningsinstituten identifiera, bedöma, övervaka och hantera alla risker till följd av arrangemang med tredje parter som de utsätts eller kan bli utsatta för, oavsett om dessa arrangemang är utkontrakteringslösningar eller inte. Riskerna med alla arrangemang med tredje parter, i synnerhet de operativa riskerna, och även de som avses i punkterna 26 och 28, bör bedömas i enlighet med avsnitt 12.2.

34. Instituten och betalningsinstituten bör säkerställa att de uppfyller alla krav enligt förordning (EU) 2016/679, inbegripet för sina avtal med tredje parter och utkontrakteringslösningar.

6 Sunda styrformer och utkontraktering

35. Utkontraktering av funktioner får inte leda till delegering av ledningsorganens ansvarsområden. Instituten och betalningsinstituten har fortfarande fullt ansvar, och kan ställas till svars, för efterlevnaden av alla sina lagstadgade skyldigheter, däribland möjligheten att kontrollera utkontrakteringen av kritiska eller viktiga funktioner.

36. Ledningsorganet har alltid fullt ansvar, och kan ställas till svars, för som minst

    a. att säkerställa att institutet eller betalningsinstitutet fortlöpande uppfyller de villkor det måste efterleva för att förbli auktoriserat, däribland alla villkor som åläggs institutet av den behöriga myndigheten,

    b. den interna organisationen av institutet eller betalningsinstitutet,

    c. att identifiera, bedöma och hantera intressekonflikter,

[22] Institut bör se kapitel V i EBA:s riktlinjer för intern styrning.

[23] Se också artikel 11 i direktiv 2015/2366 (PSD2).

[24] Se även EBA:s riktlinjer för IKT och säkerhetsriskhantering (https://eba.europa.eu/-/eba-consults-on-guidelines-on-ict-and-security-risk-management) och G7:s grunder för hantering av it-risker för tredje part i finanssektorn (https://ec.europa.eu/info/publications/g7-fundamental-elements-cybersecurity-financial-sector_en).

d. att upprätta institutets eller betalningsinstitutets strategier och principer (t.ex. affärsmodellen, riskaptiten, ramverket för riskhantering),

e. att kontrollera den dagliga förvaltningen av institutet eller betalningsinstitutet, däribland hanteringen av alla risker i samband med utkontraktering,

f. ledningsorganets kontrollerande roll i dess tillsynsfunktion, däribland att kontrollera och övervaka ledningens beslutsfattande.

37. Utkontraktering bör inte innebära en sänkning av de lämplighetskrav som tillämpas på medlemmarna i ett instituts ledningsorgan, dess direktörer och ansvariga för förvaltningen av betalningsinstitutet samt viktiga funktionsinnehavare. Instituten och betalningsinstituten bör ha fullgod kompetens samt tillräckliga och lämpligt kompetenta resurser för att säkerställa lämplig förvaltning och tillsyn av utkontrakteringslösningarna.

38. Instituten och betalningsinstituten bör

a. tydligt tilldela ansvarsområdena för dokumentationen, förvaltningen och kontrollen av utkontrakteringslösningar,

b. tilldela tillräckliga resurser för att säkerställa efterlevnad av alla juridiska krav och regleringskrav, däribland dessa riktlinjer, och dokumentation och övervakning av alla utkontrakteringslösningar,

c. med hänsyn till avsnitt 1 i dessa riktlinjer upprätta en utkontrakteringsfunktion eller utse en medarbetare i högre ställning som är direkt ansvarig inför ledningsorganet (t.ex. en ledande innehavare av en kontrollfunktion) och har ansvar för att förvalta och kontrollera riskerna med utkontrakteringslösningar som en del i institutets ram för intern kontroll, och har tillsyn över dokumentationen av utkontrakteringslösningarna. Små och mindre komplexa institut eller betalningsinstitut bör som minst säkerställa en tydlig uppdelning av uppgifter och ansvar för förvaltningen och kontrollen av utkontrakteringslösningar, och kan tilldela utkontrakteringsfunktionen till en ledamot i institutets eller betalningsinstitutets ledningsorgan.

39. Instituten och betalningsinstituten bör alltid hålla en tillräcklig substans och inte bli ”tomma skal” eller ”brevlådeföretag”. För detta ändamål bör de

a. alltid uppfylla villkoren för sin auktorisation [25], inklusive att ledningsorganet ändamålsenligt utför sina ansvarsområden enligt beskrivningen i punkt 36 i dessa riktlinjer,

[25] Se även de tekniska standarderna för tillsyn enligt artikel 8.2 i direktiv 2013/36/EU om vilken information som ska lämnas för auktorisering av kreditinstitut, och de tekniska standarderna för genomförande enligt artikel 8.3 i direktiv 2013/36/EU om standardformulär, mallar och förfaranden för att lämna den information som krävs för att auktorisera kreditinstitut (https://eba.europa.eu/regulation-and-policy/other-topics/rts-and-its-on-the-authorisation-of-credit-institutions).

b. behålla en tydlig och öppen organisatorisk ramverk och struktur som gör att de kan säkerställa efterlevnad av juridiska krav och regleringskrav,

c. när interna kontrollfunktioners operativa uppgifter utkontrakteras (t.ex. i händelse av utkontraktering inom en grupp eller utkontraktering inom institutionella skyddssystem), utöva lämplig tillsyn och kunna hantera de risker som uppkommer genom utkontraktering av kritiska eller viktiga funktioner,

d. ha tillräckliga resurser och kapacitet för att säkerställa efterlevnad av led a till c.

40. Vid utkontraktering bör instituten och betalningsinstituten som minst säkerställa att

a. de kan fatta och genomföra beslut som gäller deras affärsverksamhet och kritiska eller viktiga funktioner, även beträffande dem som har utkontrakterats,

b. de behåller ordningen i utförandet av sin affärsverksamhet och de bank- och betalningstjänster de tillhandahåller,

c. de risker som förknippas med nuvarande och planerade utkontrakteringslösningar blir tillräckligt identifierade, bedömda, hanterade och mildrade, däribland risker som rör IKT och finansteknik,

d. lämpliga sekretessarrangemang finns inrättade när det gäller uppgifter och annan information,

e. ett lämpligt flöde av relevant information med tjänsteleverantörer upprätthålls,

f. de kan, när det gäller utkontraktering av kritiska eller viktiga funktioner, inom en lämplig tidsram genomföra minst en av åtgärderna att

   i. överföra funktionen till alternativa tjänsteleverantörer,

   ii. återinföra funktionen, eller

   iii. upphöra med de affärsverksamheter som är beroende av funktionen,

g. när personuppgifter behandlas av tjänsteleverantörer som befinner sig i EU och/eller tredjeländer, lämpliga åtgärder genomförs och uppgifter behandlas i enlighet med förordning (EU) 2016/679.

För betalningsinstitut, se EBA:s riktlinjer enligt direktiv (EU) 2015/2366 (PSD2) om vilken information som ska lämnas för auktorisation av betalningsinstitut och institut för elektroniska pengar och för registrering av leverantörer av kontoinformationstjänster (https://eba.europa.eu/documents/10180/2015792/Guidelines+on+Authorisations+of+Payment+Institutions+%28EBA-GL-2017-09%29_SV.pdf/aa3a034b-6345-4f60-8598-29b2f6a27421).

7 Policy för utkontraktering

41. Ledningsorganet för ett institut eller betalningsinstitut[26] som har utkontrakteringslösningar inrättade eller planer på att börja med sådana utkontrakteringslösningar bör godkänna, regelbundet granska och uppdatera en skriftlig policy för utkontraktering och säkerställa att den genomförs, efter vad som är tillämpligt, på individuell nivå, undergruppsnivå och gruppnivå. För institut bör utkontrakteringspolicyn vara i enlighet med avsnitt 8 i EBA:s riktlinjer för intern styrning, och bör i synnerhet ta hänsyn till de krav som fastställs i avsnitt 18 i dessa riktlinjer (nya produkter och väsentliga förändringar). Betalningsinstitut kan också anpassa sina policyer efter avsnitt 8 och 18 i EBA:s riktlinjer för intern styrning.

42. Policyn bör innefatta huvudfaserna i utkontrakteringslösningarnas livscykel och innehålla definitioner av principerna, ansvarsområdena och processerna som gäller utkontraktering. I synnerhet bör policyn minst omfatta

    a. ansvarsområdena för ledningsorganet i enlighet med punkt 36, däribland, efter vad som är lämpligt, dess inblandning i beslutsfattandet om utkontraktering av kritiska eller viktiga funktioner,

    b. involveringen av affärsområden, interna kontrollfunktioner och andra enskilda personer när det gäller utkontrakteringslösningar,

    c. planeringen av utkontrakteringslösningar, inbegripet

        i. definitionen av affärsmässiga krav beträffande utkontrakteringslösningar,

        ii. kriterierna, däribland dem som avses i avsnitt 4, och processerna för att identifiera kritiska eller viktiga funktioner,

        iii. identifiering, bedömning och hantering av risker i enlighet med avsnitt 12.2,

        iv. företagsbesiktning av blivande tjänsteleverantörer, däribland de åtgärder som krävs enligt avsnitt 12.3,

        v. förfaranden för att identifiera, bedöma, förvalta och mildra potentiella intressekonflikter, i enlighet med avsnitt 8,

        vi. planering av affärskontinuitet i enlighet med avsnitt 9,

        vii. godkännandeprocessen för nya utkontrakteringslösningar,

    d. genomförandet, övervakningen och förvaltningen av utkontrakteringslösningar, däribland

[26] Se även EBA:s riktlinjer om säkerhetsåtgärder för operativa risker och säkerhetsrisker vid betaltjänster enligt PSD2, som finns under: https://www.eba.europa.eu/regulation-and-policy/payment-services-and-electronic-money/guidelines-on-security-measures-for-operational-and-security-risks-under-the-psd2

i. den fortgående bedömningen av tjänsteleverantörens resultat i enlighet med avsnitt 14,

ii. förfarandena för att få anmälan om och svara på ändringar av en utkontrakteringslösning eller tjänsteleverantör (t.ex. ändringar av dess finansiella position, organisations- eller ägarstruktur, under-utkontraktering),

iii. den oberoende granskningen och revisionen av efterlevnad av juridiska krav och regleringskrav och policyer,

iv. förnyandeprocesserna,

e. dokumentationen och registerföringen, med hänsyn till kraven i avsnitt 11,

f. exitstrategierna och uppsägningsprocesserna, däribland ett krav på en dokumenterad exitplan för varje kritisk eller viktig funktion som ska utkontrakteras när ett sådant utträde anses möjligt med hänsyn till möjliga tjänsteavbrott eller oväntad uppsägning av en utkontrakteringslösning.

43. I policyn för utkontraktering bör det göras åtskillnad mellan följande:

a. Utkontraktering av kritiska eller viktiga funktioner och andra utkontrakteringslösningar.

b. Utkontraktering till tjänsteleverantörer som är auktoriserade av en behörig myndighet och till tjänsteleverantörer som inte är det.

c. Utkontrakteringslösningar inom en grupp, utkontrakteringslösningar inom samma institutionella skyddssystem (inbegripet enheter som helt ägs individuellt eller kollektivt av institut inom det institutionella skyddssystemet) och utkontraktering till enheter utanför gruppen.

d. Utkontraktering till tjänsteleverantörer som är etablerade i en medlemsstat och tjänsteleverantörer i tredjeländer.

44. Instituten och betalningsinstituten bör säkerställa att policyn omfattar identifiering av följande potentiella effekter av kritiska eller viktiga utkontrakteringslösningar och att hänsyn tas till dessa i beslutsprocessen:

a. Institutets riskprofil.

b. Förmågan att kontrollera tjänsteleverantören och hantera riskerna.

c. Affärskontinuitetsåtgärderna.

d. Utförandet av deras affärsverksamhet.

8 Intressekonflikter

45. Institut, i enlighet med kapitel I, avsnitt 11 i EBA:s riktlinjer för intern styrning [27], och betalningsinstitut ska identifiera, bedöma och hantera intressekonflikter när det gäller deras utkontrakteringslösningar.

46. När utkontraktering ger upphov till väsentliga intressekonflikter, inbegripet mellan enheter inom samma grupp eller institutionella skyddssystem, behöver instituten och betalningsinstituten vidta lämpliga åtgärder för att hantera dessa intressekonflikter.

47. När funktioner tillhandahålls av en tjänsteleverantör som ingår i en grupp eller är medlem i ett institutionellt skyddssystem eller som ägs av det institut, det betalningsinstitut, den grupp eller de institut som är medlemmar i ett institutionellt skyddssystem, bör villkoren, inklusive de finansiella villkoren, för den utkontrakterade tjänsten sättas enligt armlängdsprincipen. När det gäller prissättningen för tjänsterna kan emellertid synergier till följd av att samma eller liknande tjänster tillhandahålls till flera institut inom en grupp eller ett institutionellt skyddssystem vara en faktor, så länge tjänsteleverantören klarar sig på fristående basis; inom en grupp bör detta gälla oavsett fallering för någon annan enhet i gruppen.

9 Affärskontinuitetsplaner

48. Institut, i enlighet med kraven i artikel 85.2 i direktiv 2013/36/EU och kapitel VI i EBA:s riktlinjer för intern styrning[28], och betalningsinstitut bör ha inrättat, upprätthålla och regelbundet pröva lämpliga affärskontinuitetsplaner när det gäller utkontrakterade kritiska eller viktiga funktioner. Institut och betalningsinstitut inom en grupp eller ett institutionellt skyddssystem kan förlita sig på centralt upprättade affärskontinuitetsplaner beträffande sina utkontrakterade funktioner.

49. I affärskontinuitetsplanerna bör hänsyn tas till eventualiteten att kvaliteten på tillhandahållandet av den utkontrakterade kritiska eller viktiga funktionen sjunker till en oacceptabel nivå eller helt uteblir. I sådana planer bör också hänsyn tas till den potentiella inverkan om tjänsteleverantörer blir insolventa eller fallerar på annat sätt, och i relevanta fall politiska risker i tjänsteleverantörens jurisdiktion.

[27] Betalningsinstitut kan också anpassa sina policyer efter dessa riktlinjer.

[28] Finns under: https://eba.europa.eu/regulation-and-policy/internal-governance/guidelines-on-internal-governance-revised-

10 Internrevisionsfunktion

50. Internrevisionsfunktionens [29] verksamhet bör med ett riskbaserat arbetssätt omfatta oberoende granskning av utkontrakterad verksamhet. Revisionsplanen[30] och programmet bör i synnerhet innefatta utkontrakteringslösningarna för kritiska eller viktiga funktioner.

51. När det gäller utkontrakteringsprocessen bör internrevisionen som minst säkerställa

    a. att institutets eller betalningsinstitutets ram för utkontraktering, inklusive utkontrakteringspolicyn, är korrekt och ändamålsenligt genomförd och i linje med tillämpliga lagar och regelverk, riskstrategin och ledningsorganets beslut,

    b. att bedömningen av om funktioner är kritiska eller viktiga är tillräcklig, kvalitativ och ändamålsenlig,

    c. att riskbedömningen för utkontrakteringslösningar är tillräcklig, kvalitativ och ändamålsenlig och att riskerna förblir i linje med institutets riskstrategi,

    d. att styrningsorganen är lämpligt involverade,

    e. lämplig övervakning och förvaltning av utkontrakteringslösningar.

11 Dokumentationskrav

52. Som en del i sitt ramverk för riskhantering bör instituten och betalningsinstituten föra ett uppdaterat register med information om alla utkontrakteringslösningar på institutet och, i tillämpliga fall, på undergruppsnivå och gruppnivå, såsom fastställs i avsnitt 2, och bör på lämpligt sätt dokumentera alla aktuella utkontrakteringslösningar, med åtskillnad mellan utkontraktering av kritiska eller viktiga funktioner och andra utkontrakteringslösningar. Med hänsyn till nationell lagstiftning bör instituten bibehålla dokumentationen som rör avslutade utkontrakteringslösningar i registret och den stödjande dokumentationen under en lämplig period.

53. Med hänsyn till kapitel I i dessa riktlinjer, och enligt de villkor som fastställs i punkt 23 d, för institut och betalningsinstitut inom en grupp, institut som är permanent underställda ett centralt organ eller institut som är medlemmar i samma institutionella skyddssystem, kan registret lagras centralt.

---

[29] Beträffande internrevisionsfunktionens ansvarsområden bör institut se avsnitt 22 i EBA:s riktlinjer för intern styrning (https://eba.europa.eu/regulation-and-policy/internal-governance/guidelines-on-internal-governance-revised-) och betalningsinstitut bör se i riktlinje 5 i EBA:s riktlinjer för auktorisation av betalningsinstitut (https://eba.europa.eu/documents/10180/2015792/Guidelines+on+Authorisations+of+Payment+Institutions+%28EBA-GL-2017-09%29_SV.pdf/aa3a034b-6345-4f60-8598-29b2f6a27421).

[30] Se även EBA:s riktlinjer för översyns- och utvärderingsprocessen: https://eba.europa.eu/regulation-and-policy/supervisory-review-and-evaluation-srep-and-pillar-2/guidelines-for-common-procedures-and-methodologies-for-the-supervisory-review-and-evaluation-process-srep-and-supervisory-stress-testing

54. Registret bör innehålla som minst följande information för alla befintliga utkontrakteringslösningar:

    a. Ett referensnummer för varje utkontrakteringslösning.

    b. Startdatum och, efter vad som är tillämpligt, datum för nästa kontraktsförnyelse, slutdatum och/eller anmälningsperioder för tjänsteleverantören och för institutet eller betalningsinstitutet.

    c. En kort beskrivning av den utkontrakterade funktionen, däribland vilka uppgifter som utkontrakteras och (t.ex. genom att ange ja eller nej i ett separat datafält) om personuppgifter har överförts eller inte eller om behandlingen av dem är utkontrakterad till en tjänsteleverantör.

    d. En kategori tilldelad av institutet eller betalningsinstitutet som återspeglar funktionens karaktär såsom beskrivs under led c (t.ex. informationsteknik (it), kontrollfunktion), i syfte att göra det lättare att identifiera olika typer av lösningar.

    e. Tjänsteleverantörens namn, organisationsnumret, identifieringskoden för juridisk person (LEI) (när sådan finns), den registrerade adressen och andra relevanta kontaktuppgifter, samt namnet på leverantörens moderföretag (om sådant finns).

    f. Det land eller de länder där tjänsten ska utföras, inklusive var uppgifterna finns (dvs. land eller region).

    g. Huruvida den utkontrakterade funktionen anses vara kritisk eller viktig (ja/nej), samt i tillämpliga fall en kort sammanfattning av skälen till att den utkontrakterade funktionen anses kritisk eller viktig.

    h. I händelse av utkontraktering till en molntjänstleverantör bör registret innehålla information om molntjänsten och distribueringsmodellerna, dvs. offentlig/privat/hybrid/community, och den särskilda karaktären på uppgifterna som ska hållas och platserna (dvs. länder eller regioner) där sådana uppgifter kommer att lagras.

    i. Datumet för den senaste bedömningen av om den utkontrakterade funktionen är kritisk eller viktig.

55. För utkontraktering av kritiska eller viktiga funktioner bör registret innehålla som minst följande ytterligare information:

    a. De institut, betalningsinstitut och andra företag som omfattas av den konsoliderade tillsynen eller det institutionella skyddssystemet, i tillämpliga fall, som använder sig av utkontrakteringen.

b. Huruvida tjänsteleverantören eller undertjänstleverantören ingår i gruppen eller är medlem i det institutionella skyddssystemet eller ägs av institut eller betalningsinstitut inom gruppen eller ägs av medlemmar i ett institutionellt skyddssystem.

c. Datumet för den senaste riskbedömningen och en kort sammanfattning av huvudresultaten.

d. Den enskilda person eller beslutande organ (t.ex. ledningsorganet) på institutet eller betalningsinstitutet som godkände utkontrakteringslösningen.

e. Den styrande lagen för utkontrakteringslösningen.

f. Datumen för de senaste och närmast planerade revisionerna, i tillämpliga fall.

g. I tillämpliga fall namnen på eventuella underentreprenörer som väsentliga delar av en kritisk eller viktig funktion utkontrakteras till i sin tur, däribland det land där underentreprenörerna är registrerade, var tjänsten kommer att utföras och i tillämpliga fall den plats (dvs. land eller region) där uppgifterna kommer att lagras.

h. Ett resultat av bedömningen av tjänsteleverantörens utbytbarhet (som lätt, svår eller omöjlig), möjligheten att återinföra en kritisk eller viktig funktion i institutet eller betalningsinstitutet eller följden av att upphöra med den kritiska eller viktiga funktionen.

i. Identifiering av alternativa tjänsteleverantörer i linje med led h.

j. Huruvida den utkontrakterade kritiska eller viktiga funktionen stöder affärsverksamheter som är tidsmässigt kritiska.

k. Den beräknade årliga budgetkostnaden.

56. Instituten och betalningsinstituten bör på begäran göra tillgängliga för den behöriga myndigheten antingen det fullständiga registret över alla befintliga utkontrakteringslösningar[31] eller specificerade avsnitt därifrån, såsom information om alla utkontrakteringslösningar som ligger under en av kategorierna som avses i led d i punkt 54 i dessa riktlinjer (t.ex. alla it-utkontrakteringslösningar). Instituten och betalningsinstituten bör lämna denna information i behandlingsbar elektronisk form (t.ex. ett gemensamt använt databasformat, kommaseparerade värden).

57. Instituten och betalningsinstituten bör på begäran göra tillgängliga för den behöriga myndigheten all information som behövs för att den behöriga myndigheten ska kunna utföra ändamålsenlig tillsyn av institutet eller betalningsinstitutet, däribland när så behövs en kopia av utkontrakteringsavtalet.

[31] Se också EBA:s riktlinjer för översyns- och utvärderingsprocessen, som finns under: https://eba.europa.eu/regulation-and-policy/supervisory-review-and-evaluation-srep-and-pillar-2

58. Institut, utan att det påverkar tillämpningen av artikel 19.6 i direktiv (EU) 2015/2366, och betalningsinstitut bör lägligt och på ett lämpligt sätt informera behöriga myndigheter eller inleda en tillsynsdialog med de behöriga myndigheterna om den planerade utkontrakteringen av kritiska eller viktiga funktioner och/eller när en utkontrakterad funktion har blivit kritisk eller viktig, och lämna som minst den information som specificeras i punkt 54.

59. Instituten och betalningsinstituten[32] bör lägligt informera behöriga myndigheter om väsentliga förändringar och/eller allvarliga händelser gällande deras utkontrakteringslösningar som kan ha väsentlig påverkan på det fortlöpande tillhandahållandet av institutets eller betalningsinstitutets affärsverksamhet.

60. Instituten och betalningsinstituten bör på lämpligt sätt dokumentera de bedömningar som görs enligt kapitel IV och resultaten av institutens fortlöpande övervakning (t.ex. tjänsteleverantörens resultat, efterlevnad av överenskomna tjänstenivåer, andra kontraktsenliga krav och regleringskrav, uppdateringar av riskbedömningen).

Kapitel IV – Utkontrakteringsprocess

12 Analys före utkontraktering

61. Innan institut och betalningsinstitut inleder någon utkontrakteringslösning, bör de

    a. bedöma om utkontrakteringslösningen gäller en kritisk eller viktig funktion, såsom beskrivs i kapitel II,

    b. bedöma om tillsynsvillkoren för utkontraktering som fastställs i avsnitt 12.1 är uppfyllda,

    c. identifiera och bedöma alla relevanta risker med utkontrakteringslösningen i enlighet med avsnitt 12.2,

    d. genomföra företagsbesiktning av den blivande tjänsteleverantören i enlighet med avsnitt 12.3,

    e. identifiera och bedöma intressekonflikter som utkontrakteringen kan orsaka i enlighet med avsnitt 8.

[32] Se även EBA:s riktlinjer för rapportering vid allvarliga incidenter enligt PSD2, som finns under: https://www.eba.europa.eu/regulation-and-policy/payment-services-and-electronic-money/guidelines-on-major-incidents-reporting-under-psd2

12.1 Tillsynsvillkor för utkontraktering

62. Institut och betalningsinstitut bör säkerställa att utkontrakteringen av bankverksamheters[33] eller betalningstjänsters funktioner, i den omfattningen att utförandet av denna funktion kräver auktorisation eller registrering av en behörig myndighet i medlemsstaten där de är auktoriserade, till en tjänsteleverantör som finns i samma eller en annan medlemsstat endast äger rum om ett av följande villkor är uppfyllt:

    a. Tjänsteleverantören är auktoriserad eller registrerad av en behörig myndighet för att utföra sådana bankverksamheter eller betalningstjänster.

    b. Tjänsteleverantören har på annat sätt tillåtelse att utföra dessa bankverksamheter eller betalningstjänster i enlighet med den relevanta nationella rättsliga ramen.

63. Institut och betalningsinstitut bör säkerställa att utkontrakteringen av bankverksamheters eller betalningstjänsters funktioner, i den omfattningen att utförandet av denna funktion kräver auktorisation eller registrering av en behörig myndighet i medlemsstaten där de är auktoriserade, till en tjänsteleverantör som finns i ett tredjeland endast äger rum om följande villkor är uppfyllda:

    a. Tjänsteleverantören är auktoriserad eller registrerad för att tillhandahålla den bankverksamheten eller betalningstjänsten i tredjelandet och har tillsyn av en relevant behörig myndighet i det tredjelandet (benämns som en ”tillsynsmyndighet”).

    b. Det finns ett lämpligt samarbetsavtal, t.ex. i form av ett samförståndsavtal eller kollegieavtal, mellan de behöriga myndigheter som ansvarar för tillsyn av institutet och de tillsynsmyndigheter som ansvarar för tillsyn av tjänsteleverantören.

    c. Samarbetsavtalet som avses i led b bör säkerställa att de behöriga myndigheterna som minst kan

        i. erhålla på begäran den information som behövs för att utföra deras tillsynsuppgifter i enlighet med direktiv 2013/36/EU, förordning (EU) nr 575/2013, direktiv (EU) 2015/2366 och direktiv 2009/110/EG,

        ii. erhålla tillräcklig tillgång till alla uppgifter, handlingar, lokaler eller personal i tredjelandet som är relevanta för att de ska kunna utöva sina tillsynsbefogenheter,

        iii. motta, så snart som möjligt, information från tillsynsmyndigheten i tredjelandet för att utreda uppenbara överträdelser av kraven i direktiv 2013/36/EU, förordning (EU) nr 575/2013, direktiv (EU) 2015/2366 och direktiv 2009/110/EG, och

[33] Se artikel 9 i kapitalkravsdirektivet när det gäller förbud för personer eller företag som inte är kreditinstitut att driva rörelse som omfattar att från allmänheten ta emot insättningar eller andra återbetalbara medel.

iv. samarbeta med de relevanta tillsynsmyndigheterna i tredjelandet om verkställighet i händelse av överträdelse av de gällande regleringskraven och den nationella lagstiftningen i medlemsstaten. Samarbetet bör bland annat innefatta att motta information om potentiella överträdelser av de gällande regleringskraven från tillsynsmyndigheterna i tredjelandet så snart som är praktiskt möjligt.

12.2 Riskbedömning av utkontrakteringslösningar

64. Institut och betalningsinstitut bör bedöma hur utkontrakteringslösningar potentiellt påverkar deras operativa risk, ta hänsyn till bedömningsresultaten när de beslutar om funktionen bör utkontrakteras till en tjänsteleverantör, och vidta lämpliga åtgärder för att undvika olämpliga ytterligare operativa risker innan de inleder utkontrakteringslösningar.

65. Bedömningen bör när så är lämpligt innehålla scenarier för möjliga riskhändelser, däribland operativa riskhändelser med hög allvarlighetsgrad. I scenarioanalysen bör instituten och betalningsinstituten bedöma den potentiella påverkan om tjänster uteblir eller är otillräckliga, inklusive de risker som orsakas av processer, system, personer eller externa händelser. Instituten och betalningsinstituten bör, med hänsyn till proportionalitetsprincipen som beskrivs i avsnitt 1, dokumentera den utförda analysen och sina resultat samt uppskatta i vilken omfattning utkontrakteringslösningen skulle öka eller minska deras operativa risk. Med hänsyn till kapitel I kan små och icke-komplexa institut och betalningsinstitut använda kvalitativa arbetssätt för riskbedömning, medan stora eller komplexa institut bör ha ett mer sofistikerat arbetssätt, däribland att i mån av tillgång använda interna och externa förlustdata som information i scenarioanalysen.

66. I riskbedömningen bör instituten och betalningsinstituten också ta hänsyn till de förväntade fördelarna och kostnaderna med den föreslagna utkontrakteringslösningen, vilket innefattar att väga eventuella risker som kan minskas eller hanteras bättre mot eventuella risker som kan uppstå till följd av den föreslagna utkontrakteringslösningen, med hänsyn som minst till

    a. koncentrationsrisker, däribland genom

        i. utkontraktering till en dominerande tjänsteleverantör som inte är lätt utbytbar, och

        ii. flera olika utkontrakteringslösningar med samma tjänsteleverantör eller tjänsteleverantörer som är nära kopplade till varandra,

    b. de sammantagna riskerna till följd av utkontraktering av flera funktioner runtom i institutet eller betalningsinstitutet och, när det gäller grupper av institut eller institutionella skyddssystem, de sammantagna riskerna på konsoliderad basis eller grundat på det institutionella skyddssystemet,

c. när det gäller betydande institut, ingripanderisken, dvs. den risk som kan uppstå genom att man behöver tillhandahålla finansiellt stöd till en tjänsteleverantör i trångmål eller ta över dess affärsverksamhet,

d. de åtgärder som införs av institutet eller betalningsinstitutet och av tjänsteleverantören för att hantera och dämpa riskerna.

67. När utkontrakteringslösningen innefattar möjligheten att tjänsteleverantören i sin tur utkontrakterar kritiska eller viktiga funktioner till andra tjänsteleverantörer, bör instituten och betalningsinstituten ta hänsyn till

a. riskerna som förknippas med vidareutkontraktering, däribland de ytterligare risker som kan uppstå om underentreprenören finns i ett tredjeland eller ett annat land än tjänsteleverantören,

b. risken för att långa och komplicerade kedjor av vidare utkontraktering minskar institutens eller betalningsinstitutens möjlighet att kontrollera den utkontrakterade kritiska eller viktiga funktionen och de behöriga myndigheternas möjlighet till ändamålsenlig tillsyn av dem.

68. När riskbedömningen utförs före utkontraktering och under pågående övervakning av tjänsteleverantörens resultat, bör instituten och betalningsinstituten som minst

a. definiera och klassificera de relevanta funktionerna och därmed förknippade uppgifter och system vad gäller känslighet och de säkerhetsåtgärder som krävs,

b. utföra en noggrann riskbaserad analys av de funktioner och därmed förknippade uppgifter och system som övervägs för utkontraktering eller har utkontrakterats, och bemöta de potentiella riskerna, i synnerhet de operativa riskerna, däribland juridiska och IKT-relaterade risker, efterlevnads- och ryktesrisker, och begränsningarna i kontrollen för de länder där de utkontrakterade tjänsterna tillhandahålls eller kan komma att tillhandahållas och där uppgifterna lagras eller sannolikt kommer att lagras,

c. beakta konsekvenserna av var tjänsteleverantören finns (inom eller utanför EU),

d. beakta den politiska stabiliteten och säkerhetssituationen i jurisdiktionerna i fråga, däribland

i. gällande lagar, inklusive lagar för dataskydd,

ii. vilka bestämmelser för brottsbekämpning som finns,

iii. den insolvenslagstiftning som skulle gälla i händelse av en tjänsteleverantörs fallering och eventuella hinder som skulle uppkomma i samband med brådskande återhämtning av i synnerhet institutets eller betalningsinstitutets uppgifter,

e. definiera och besluta om en lämplig skyddsnivå för datasekretessen, om kontinuiteten för de verksamheter som ska utkontrakteras, och om integriteten och spårbarheten för data och system mot bakgrund av den avsedda utkontrakteringen; instituten och betalningsinstituten bör också överväga att vidta särskilda åtgärder om så behövs för transiterande, minnesbelägna och vilande data, såsom användningen av krypteringstekniker i kombination med en lämplig nyckelhanteringsarkitektur,

f. beakta om tjänsteleverantören är ett dotterföretag eller moderföretag till institutet, omfattas av sammanställd redovisning eller är medlem i eller ägs av institut som är medlemmar i ett institutionellt skyddssystem och, i så fall, i hur hög grad institutet kontrollerar den eller har möjlighet att påverka dess åtgärder i linje med avsnitt 2.

12.3 Företagsbesiktning

69. Innan institut och betalningsinstitut inleder en utkontrakteringslösning och beaktar de operativa riskerna i samband med funktionen som ska utkontrakteras, bör de säkerställa i sin urvals- och bedömningsprocess att tjänsteleverantören är lämplig.

70. När det gäller kritiska och viktiga funktioner, bör instituten och betalningsinstituten säkerställa att tjänsteleverantören har affärsmässigt rykte, lämpliga och tillräckliga förmågor, expertis, kapacitet, resurser (t.ex. personal, it, ekonomi), organisationsstruktur och i tillämpliga fall de lagstadgade auktorisationer eller registreringar som krävs för att utföra den kritiska eller viktiga funktionen på ett tillförlitligt och professionellt sätt så den kan uppfylla sina skyldighet så länge kontraktsförslaget varar.

71. Ytterligare faktorer att ta hänsyn till när man utför företagsbesiktning av en potentiell tjänsteleverantör är bland annat

    a. dess affärsmodell, karaktär, omfattning, komplexitet, finansiella situation, ägarstruktur och gruppstruktur,

    b. de långsiktiga relationerna med tjänsteleverantörer som redan har bedömts och utför tjänster för institutet eller betalningsinstitutet,

    c. om tjänsteleverantören är ett moderföretag eller dotterföretag till institutet eller betalningsinstitutet, ingår i institutets sammanställda redovisning eller är medlem i eller ägs av institut som är medlemmar i samma institutionella skyddssystem som institutet hör till,

    d. om tjänsteleverantören har tillsyn av behöriga myndigheter eller inte.

72. När utkontrakteringen innefattar behandling av personuppgifter eller konfidentiella uppgifter, bör instituten och betalningsinstituten förvissa sig om att tjänsteleverantören inför lämpliga tekniska och organisatoriska åtgärder för att skydda uppgifterna.

73. Instituten och betalningsinstituten bör vidta lämpliga åtgärder för att säkerställa att tjänsteleverantörerna agerar på ett sätt som överensstämmer med deras värderingar och uppförandekod. I synnerhet när det gäller tjänsteleverantörer som finns i tredjeländer, och i tillämpliga fall deras underentreprenörer, bör instituten och betalningsinstituten förvissa sig om att tjänsteleverantören agerar på ett etiskt och socialt ansvarsfullt sätt och följer internationella människorättsnormer (t.ex. Europeiska konventionen om mänskliga rättigheter), miljöskydd och lämpliga arbetsförhållanden, inklusive förbud mot barnarbete.

13 Kontraktsfasen

74. Institutets, betalningsinstitutets och tjänsteleverantörens rättigheter och skyldigheter ska fördelas tydligt och fastställas i ett skriftligt avtal.

75. I utkontrakteringsavtalet för kritiska eller viktiga funktioner bör som minst följande fastställas:

    a. En tydlig beskrivning av den utkontrakterade funktionen som ska tillhandahållas.

    b. Startdatum och slutdatum, i tillämpliga fall, för avtalet och anmälningsperioderna för tjänsteleverantören och institutet eller betalningsinstitutet.

    c. Den styrande lagen för avtalet.

    d. Parternas finansiella skyldigheter.

    e. Huruvida vidare utkontraktering av en kritisk eller viktig funktion, eller väsentliga delar därav, är tillåten och i så fall de villkor i avsnitt 13.1 som den vidare utkontrakteringen är underställd.

    f. Platsen/platserna (dvs. regioner eller länder) där den kritiska eller viktiga funktionen kommer att tillhandahållas och/eller där relevanta uppgifter kommer att förvaras och behandlas, inklusive den möjliga lagringsplatsen, och de villkor som ska uppfyllas, inklusive ett krav på att meddela institutet eller betalningsinstitutet om tjänsteleverantören föreslår att platsen/platserna ändras.

    g. I relevanta fall villkor gällande tillgänglighet, åtkomlighet, integritet, sekretess och säkerhet för relevanta uppgifter, enligt vad som anges i avsnitt 13.2.

    h. Institutets eller betalningsinstitutets rätt att fortlöpande övervaka tjänsteleverantörens resultat.

    i. De överenskomna tjänstenivåerna, som bör inkludera exakta kvantitativa och kvalitativa resultatmål för den utkontrakterade funktionen för att möjliggöra läglig övervakning så att lämpliga korrigerande åtgärder kan vidtas utan onödigt dröjsmål om de överenskomna tjänstenivåerna inte uppfylls.

j. Tjänsteleverantörens rapporteringsskyldigheter till institutet eller betalningsinstitutet, däribland kommunikation från tjänsteleverantören om all utveckling som kan ha väsentlig påverkan på tjänsteleverantörens förmåga att ändamålsenligt utföra den kritiska eller viktiga funktionen enligt de överenskomna tjänstenivåerna och i överensstämmelse med gällande lag och regleringskrav, och efter vad som är lämpligt skyldigheter att lämna in rapporter om tjänsteleverantörens internrevisionsfunktion.

k. Huruvida tjänsteleverantören bör teckna en obligatorisk försäkring mot vissa risker och, i tillämpliga fall, vilken nivå på försäkringsskydd som efterfrågas.

l. Kraven på att införa och pröva affärskontinuitetsplaner.

m. Villkor som säkerställer att de uppgifter som ägs av institutet eller betalningsinstitutet går att få tillgång till i händelse av insolvens, resolution eller upphörd affärsverksamhet för tjänsteleverantören.

n. Tjänsteleverantörens skyldighet att samarbeta med institutets eller betalningsinstitutets behöriga myndigheter och resolutionsmyndigheter, däribland andra personer som utsetts av dem.

o. För institut en tydlig hänvisning till den nationella resolutionsmyndighetens befogenheter, särskilt till artiklarna 68 och 71 i direktiv 2014/59/EU (direktivet om inrättande av en ram för återhämtning och resolution av kreditinstitut och värdepappersföretag) och i synnerhet en beskrivning av de ”väsentliga förpliktelserna” i kontraktet i den mening som avses i artikel 68 i det direktivet.

p. Den obegränsade rättigheten för institut, betalningsinstitut och behöriga myndigheter att inspektera och granska tjänsteleverantören i synnerhet med avseende på den kritiska eller viktiga utkontrakterade funktionen, såsom anges i avsnitt 13.3.

q. Uppsägningsrättigheter, såsom anges i avsnitt 13.4.

13.1 Vidare utkontraktering av kritiska eller viktiga funktioner

76. I utkontrakteringsavtalet bör det anges om det är tillåtet eller inte att vidare utkontraktera kritiska eller viktiga funktioner, eller väsentliga delar av dem.

77. Om vidare utkontraktering av kritiska eller viktiga funktioner är tillåten, bör instituten och betalningsinstituten avgöra om den del av funktionen som ska utkontrakteras vidare som sådan är kritisk eller viktig (dvs. en väsentlig del av den kritiska eller viktiga funktionen) och i så fall dokumentera den i registret.

78. Om vidare utkontraktering av kritiska eller viktiga funktioner är tillåten, bör det i det skriftliga avtalet

a. anges alla typer av verksamhet som är undantagna från vidare utkontraktering,

b. anges de villkor som ska följas i händelse av vidare utkontraktering,

c. anges att tjänsteleverantören är skyldig att kontrollera de tjänster som den har utkontrakterat vidare, för att säkerställa att alla kontraktsförpliktelser mellan tjänsteleverantören och institutet eller betalningsinstitutet kontinuerligt uppfylls,

d. krävas att tjänsteleverantören erhåller föregående särskilt eller allmänt skriftligt tillstånd från institutet eller betalningsinstitutet innan uppgifter utkontrakteras vidare[34],

e. ingå en skyldighet för tjänsteleverantören att informera institutet eller betalningsinstitutet om varje planerad vidare utkontraktering, eller väsentliga ändringar därav, i synnerhet när detta kan påverka tjänsteleverantörens förmåga att uppfylla sina ansvarsområden enligt utkontrakteringsavtalet; detta innefattar planerade väsentliga byten av underentreprenörer och av anmälningsperioden; i synnerhet bör den anmälningsperiod som ska fastställas ha utrymme för det utkontrakterande institutet eller betalningsinstitutet att åtminstone utföra en riskbedömning av de föreslagna ändringarna och invända mot ändringar innan den planerade vidare utkontrakteringen, eller väsentliga ändringar av den, börjar gälla,

f. säkerställas i lämpliga fall att institutet eller betalningsinstitutet har rätt att invända mot avsedd vidare utkontraktering eller väsentliga ändringar därav, eller att uttryckligt godkännande krävs,

g. säkerställas att institutet eller betalningsinstitutet har den kontraktsmässiga rätten att säga upp avtalet i händelse av otillbörlig vidare utkontraktering, t.ex. när den vidare utkontrakteringen avsevärt ökar riskerna för institutet eller betalningsinstitutet eller när tjänsteleverantören utkontrakterar vidare utan att meddela institutet eller betalningsinstitutet om detta.

79. Instituten och betalningsinstituten bör godkänna vidare utkontraktering endast om underentreprenören åtar sig att

    a. följa alla tillämpliga lagar, regleringskrav och kontraktsmässiga skyldigheter,

    b. bevilja institutet, betalningsinstitutet och den behöriga myndigheten samma kontraktsmässiga rättigheter till åtkomst och revision som dem som beviljas av tjänsteleverantören.

80. Instituten och betalningsinstituten bör säkerställa att tjänsteleverantören ordentligt kontrollerar de underställda tjänsteleverantörerna, i enlighet med den policy som definieras av institutet eller betalningsinstitutet. Om den föreslagna vidare utkontrakteringen skulle kunna få väsentlig negativ inverkan på utkontrakteringslösningen för en kritisk eller viktig funktion eller skulle leda till en avsevärt ökad risk, däribland när villkoren i punkt 79 inte skulle uppfyllas,

[34] Se artikel 28 i förordning (EU) 2016/679.

bör institutet eller betalningsinstitutet utöva sin rätt att invända mot den vidare utkontrakteringen, om en sådan rätt var avtalad, och/eller säga upp kontraktet.

13.2 Data- och systemsäkerhet

81. Institut och betalningsinstitut bör säkerställa att tjänsteleverantörer när det är relevant följer lämpliga it-säkerhetsstandarder.

82. När det är relevant (t.ex. i samband med utkontraktering av moln eller annan IKT) bör instituten och betalningsinstituten definiera data- och systemsäkerhetskrav i utkontrakteringsavtalet och fortlöpande övervaka efterlevnad av dessa krav.

83. I fall av utkontraktering till molntjänstleverantörer och andra utkontrakteringslösningar som inbegriper hantering eller överföring av personuppgifter eller konfidentiella uppgifter, bör instituten och betalningsinstituten anta ett riskbaserat förhållningssätt till platsen/platserna för datalagring och behandling av uppgifter (dvs. land eller region) och beakta informationssäkerheten.

84. Utan att det påverkar tillämpningen av kraven enligt förordning (EU) 2016/679, bör instituten och betalningsinstituten vid sin utkontraktering (i synnerhet till tredjeländer) ta hänsyn till skillnader i nationella bestämmelser när det gäller skydd av uppgifter. Instituten och betalningsinstituten bör säkerställa att utkontrakteringsavtalet innehåller skyldigheten för tjänsteleverantören att skydda konfidentiell, personlig eller på annat sätt känslig information och följa alla juridiska krav på dataskydd som gäller för institutet eller betalningsinstitutet (t.ex. skydd av personuppgifter och att banksekretess eller liknande rättsliga konfidentialitetsplikter för kunders information, i tillämpliga fall, iakttas).

13.3 Åtkomst-, informations- och revisionsrättigheter

85. Institut och betalningsinstitut bör säkerställa i det skriftliga arrangemanget för utkontrakteringen att internrevisionsfunktionen kan granska den utkontrakterade funktionen genom ett riskbaserat arbetssätt.

86. Oavsett hur kritisk eller viktig den utkontrakterade funktionen är, ska de skriftliga utkontrakteringsarrangemangen mellan institut och tjänsteleverantörer hänvisa till behöriga myndigheters och resolutionsmyndigheters befogenheter för informationsinhämtning och utredning enligt artikel 63.1 a i direktiv 2014/59/EU och artikel 65.3 i direktiv 2013/36/EU när det gäller tjänsteleverantörer som finns i en medlemsstat, och bör också säkerställa dessa rättigheter när det gäller tjänsteleverantörer som finns i tredjeländer.

87. När det gäller utkontraktering av kritiska eller viktiga funktioner, bör instituten och betalningsinstituten säkerställa i det skriftliga utkontrakteringsavtalet att tjänsteleverantören beviljar dem och deras behöriga myndigheter, inklusive resolutionsmyndigheter, och alla andra personer som utnämnts av dem eller de behöriga myndigheterna, följande:

a. Fullständigt tillträde till alla relevanta företagslokaler (t.ex. huvudkontor och operativa centraler), inklusive hela utbudet av relevanta enheter, system, nätverk, information och uppgifter som används för att tillhandahålla den utkontrakterade funktionen, däribland anknuten finansiell information, personal och tjänsteleverantörens utomstående revisorer (”åtkomst- och informationsrättigheter”).

b. Obegränsad rätt till inspektion och revision gällande utkontrakteringslösningen (”revisionsrättigheter”) så att de kan övervaka utkontrakteringslösningen och säkerställa att alla tillämpliga lagstadgade och kontraktsenliga krav efterlevs.

88. Vid utkontraktering av funktioner som inte är kritiska eller viktiga, bör instituten och betalningsinstituten säkerställa åtkomst- och revisionsrättigheter enligt vad som fastställs i punkt 87 a och b och avsnitt 13.3, enligt ett riskbaserat arbetssätt, med hänsyn till den utkontrakterade funktionens karaktär och de tillhörande operativa riskerna och ryktesriskerna, dess skalbarhet, den potentiella inverkan på det kontinuerliga utförandet av dess verksamhet samt kontraktsperioden. Instituten och betalningsinstituten bör ta hänsyn till att funktioner kan bli kritiska eller viktiga med tiden.

89. Instituten och betalningsinstituten bör säkerställa att utkontrakteringsavtalet eller eventuellt annat kontraktsmässigt avtal inte försämrar eller begränsar det effektiva utövandet av åtkomst- och revisionsrättigheterna för dem själva, behöriga myndigheter eller tredje parter som utsetts av dem för att utöva dessa rättigheter.

90. Instituten och betalningsinstituten bör utöva sina åtkomst- och revisionsrättigheter, bestämma hur ofta revisioner ska ske och områden som ska granskas utifrån ett riskbaserat arbetssätt samt följa relevanta och gemensamt godtagna nationella och internationella revisionsstandarder.[35]

91. Utan att det påverkar deras slutliga ansvar för utkontrakteringslösningar kan instituten och betalningsinstituten använda

a. gemensamma revisioner som organiseras tillsammans med andra kunder till samma tjänsteleverantör och som utförs av dem och dessa kunder eller av en tredje part som har utsetts av dem, för att revisionsresurserna ska utnyttjas mer effektivt och för att minska den organisatoriska bördan, både för kunden och tjänsteleverantören,

b. tredjepartscertifieringar och tredjepartsrevisionsrapporter eller interna revisionsrapporter som har gjorts tillgängliga av tjänsteleverantören.

92. Vid utkontraktering av kritiska eller viktiga funktioner bör instituten och betalningsinstituten bedöma om de tredjepartscertifieringar och tredjepartsrapporter som avses i punkt 91 b är

[35] För institut, se avsnitt 22 i EBA:s riktlinjer för intern styrning: https://eba.europa.eu/documents/10180/2164689/Guidelines+on+Internal+Governance+%28EBA-GL-2017-11%29_SV.pdf/7c81379f-32cf-488d-b034-92387fec4f2f

adekvata och tillräckliga för att uppfylla deras lagstadgade skyldigheter, och bör inte varaktigt förlita sig enbart på dessa rapporter.

93. Instituten och betalningsinstituten bör använda sig av metoden som avses i punkt 91 b endast om de

    a. är nöjda med revisionsplanen för den utkontrakterade funktionen,

    b. ser till att certifieringen eller revisionsrapporten omfattar de system (dvs. processer, applikationer, infrastruktur, datacenter osv.) och de viktiga kontroller som identifierats av institutet eller betalningsinstitutet samt efterlevnad av relevanta regleringskrav,

    c. noggrant fortlöpande bedömer innehållet i certifieringarna eller revisionsrapporterna och kontrollerar att rapporterna eller certifieringarna inte är inaktuella,

    d. säkerställer att centrala system och kontroller omfattas i framtida versioner av certifieringen eller revisionsrapporten,

    e. är tillfreds med den certifierande eller granskande partens lämplighet (t.ex. med avseende på rotationen inom certifierings- eller revisionsföretaget, kvalifikationerna, expertisen, de upprepade kontrollerna/verifieringen av bevisen i den underliggande revisionsdokumentationen),

    f. är tillfreds med att certifieringarna utfärdas och revisionerna utförs på grundval av allmänt erkända och relevanta professionella standarder och inbegriper ett test av den operativa effektiviteten hos de centrala kontroller som har införts,

    g. har den kontraktsmässiga rätten att begära att omfattningen av certifieringarna eller revisionsrapporterna utökas till andra relevanta system och kontroller; antalet sådana begäranden om ändrad omfattning och hur ofta de görs bör vara rimligt och motiverat ur ett riskhanteringsperspektiv, och

    h. behålla den kontraktsmässiga rätten att utföra individuella revisioner efter sitt omdöme med avseende på utkontraktering av kritiska eller viktiga funktioner.

94. I enlighet med EBA:s riktlinjer om IKT-riskbedömning inom ramen för ÖUP bör institut, när det är relevant, säkerställa att de kan utföra stickprov av säkerheten för att bedöma ändamålsenligheten för införda åtgärder och processer för it-säkerhet och intern IKT-säkerhet.[36] Med hänsyn till kapitel I bör betalningsinstitut också ha mekanismer för intern IKT-kontroll, däribland IKT-säkerhetskontroll och begränsningsåtgärder.

95. Innan ett planerat besök på plats äger rum bör institut, betalningsinstitut, behöriga myndigheter och revisorer eller tredje parter som agerar åt institutet, betalningsinstitutet eller

[36] Se även EBA:s riktlinjer om IKT-riskbedömning: https://eba.europa.eu/documents/10180/1954038/Guidelines+on+ICT+Risk+Assessment+under+SREP+%28EBA-GL-2017-05%29_SV.pdf/32eff4f9-7607-4b39-b128-02b0030e2ea8

behöriga myndigheter skäligen meddela detta till tjänsteleverantören, såvida inte detta är omöjligt pga. nödfall eller krissituation eller skulle leda till en situation där revisionen inte längre skulle vara ändamålsenlig.

96. När revisioner utförs i miljöer med flera klienter, bör man vara noga med att säkerställa att risker för en annan klients miljö (t.ex. inverkan på tjänstenivåer, tillgång till uppgifter, sekretessaspekter) undviks eller begränsas.

97. När utkontrakteringslösningen medför teknisk komplexitet på hög nivå, till exempel i fall med utkontraktering av molntjänster, bör institutet eller betalningsinstitutet verifiera att de personer som utför revisionen – dess interna revisorer, gemensamma revisorer eller utomstående revisorer som agerar på dess vägnar – har lämplig och relevant kompetens och kunskap för att ändamålsenligt utföra relevanta revisioner och/eller bedömningar. Samma sak gäller för all personal på institutet eller betalningsinstitutet som granskar tredjepartscertifieringar eller tredjepartsrevisioner som utförs av tjänsteleverantörer.

13.4 Uppsägningsrätt

98. Utkontrakteringslösningen bör uttryckligen tillåta möjligheten att institutet eller betalningsinstitutet säger upp lösningen, i enlighet med gällande lagstiftning, däribland i följande situationer:

    a. När leverantören av de utkontrakterade funktionerna bryter mot gällande lagstiftning, regelverk eller kontraktsvillkor.

    b. När försämringar som kan ändra den utkontrakterade funktionens resultat konstateras.

    c. När det sker väsentliga förändringar som påverkar utkontrakteringslösningen eller tjänsteleverantören (t.ex. vidare utkontraktering eller byte av underentreprenörer).

    d. När det finns svagheter beträffande förvaltningen av och säkerheten för konfidentiella, personliga eller på annat sätt känsliga data och uppgifter.

    e. När instruktioner ges av institutets eller betalningsinstitutets behöriga myndighet, t.ex. i händelse av att den behöriga myndigheten till följd av utkontrakteringslösningen inte längre är i den ställningen att den ändamålsenligt kan ha tillsyn över institutet eller betalningsinstitutet.

99. Utkontrakteringslösningen bör underlätta överföring av den utkontrakterade funktionen till en annan tjänsteleverantör eller att den återinförs till institutet eller betalningsinstitutet. För detta ändamål bör det i det skriftliga utkontrakteringsarrangemanget

    a. tydligt fastställas vilka skyldigheter den befintliga tjänsteleverantören har, i händelse av att den utkontrakterade funktionen överförs till en annan tjänsteleverantör eller

tillbaka till institutet eller betalningsinstitutet, däribland när det gäller behandling av uppgifter,

b. fastställas en lämplig övergångsperiod, under vilken tjänsteleverantören, efter uppsägning av utkontrakteringsarrangemanget, skulle fortsätta tillhandahålla den utkontrakterade funktionen för att minska risken för störningar, och

c. ingå en skyldighet för tjänsteleverantören att stödja institutet eller betalningsinstitutet med den välordnade överföringen av funktionen i händelse av att utkontrakteringsavtalet sägs upp.

14 Kontroll av utkontrakterade funktioner

100. Institut och betalningsinstitut bör fortlöpande övervaka tjänsteleverantörernas resultat sett till alla utkontrakteringslösningar, med ett riskbaserat arbetssätt och med huvudfokus på utkontrakteringen av kritiska eller viktiga funktioner, däribland att tillgängligheten, integriteten och säkerheten för uppgifter och information säkerställs. När risken, karaktären eller omfattningen för en utkontrakterad funktion har förändrats väsentligt, bör instituten och betalningsinstituten omvärdera hur kritisk eller viktig den funktionen är, i enlighet med avsnitt 4.

101. Instituten och betalningsinstituten bör tillämpa vederbörlig kompetens, försiktighet och omsorg när de övervakar och förvaltar utkontrakteringslösningar.

102. Institut bör regelbundet uppdatera sin riskbedömning i enlighet med avsnitt 12.2 och bör regelbundet rapportera till ledningsorganet om de risker som konstateras när det gäller utkontraktering av kritiska eller viktiga funktioner.

103. Instituten och betalningsinstituten bör övervaka och hantera sina interna koncentrationsrisker som orsakas av utkontrakteringslösningar, med hänsyn till avsnitt 12.2 i dessa riktlinjer.

104. Instituten och betalningsinstituten bör fortlöpande säkerställa att utkontrakteringslösningarna, med huvudfokus på utkontrakterade kritiska eller viktiga funktioner, uppfyller lämpliga standarder för resultat och kvalitet i enlighet med sina policyer, genom att

a. säkerställa att de mottar lämpliga rapporter från tjänsteleverantörer,

b. bedöma tjänsteleverantörernas resultat med hjälp av verktyg som nyckeltal för verksamheten, nyckeltal för kontroll, rapporter om tjänsteutförande, egencertifiering och oberoende granskningar,

c. granska all annan relevant information som mottas från tjänsteleverantören, däribland rapporter om affärskontinuitetsåtgärder och -prövningar.

105. Institut bör vidta lämpliga åtgärder om de konstaterar brister i tillhandahållandet av den utkontrakterade funktionen. I synnerhet bör instituten och betalningsinstituten följa upp alla eventuella indikationer på att tjänsteleverantörer kanske inte utför den utkontrakterade kritiska eller viktiga funktionen ändamålsenligt eller i enlighet med tillämpliga lagar och regleringskrav. Om brister konstateras bör instituten och betalningsinstituten vidta lämpliga korrigerande eller avhjälpande åtgärder. Sådana åtgärder kan innefatta att säga upp utkontrakteringsavtalet, med omedelbar verkan vid behov.

15 Exitstrategier

106. Institut och betalningsinstitut bör när de utkontrakterar kritiska eller viktiga funktioner ha en dokumenterad exitstrategi, som är i linje med deras utkontrakteringspolicy och affärskontinuitetsplaner[37], och där de beaktar som minst möjligheten

a. att utkontrakteringsavtalen sägs upp,

b. att tjänsteleverantören fallerar,

c. att kvaliteten på den tillhandahållna funktionen försämras och det sker eller kan ske verksamhetsstörningar till följd av att funktionen tillhandahålls otillräckligt eller inte alls,

d. att väsentliga risker uppkommer för att funktionen ska tillämpas ordentligt och kontinuerligt.

107. Instituten och betalningsinstituten bör säkerställa att de kan utträda ur utkontrakteringslösningar utan onödig störning för sina affärsverksamheter, utan att det begränsar deras efterlevnad av regleringskrav och utan någon försämring av kontinuiteten och kvaliteten när det gäller tillhandahållandet av tjänster till kunder. För att uppnå detta bör de

a. ta fram och genomföra exitplaner som är omfattande, dokumenterade och där så är lämpligt tillräckligt prövade (t.ex. genom att man utför en analys av de potentiella kostnaderna, följderna, resurserna och tidsmässiga konsekvenserna av att en utkontrakterad tjänst överförs till en alternativ leverantör),

b. identifiera alternativa lösningar och ta fram övergångsplaner så att institutet eller betalningsinstitutet kan ta bort utkontrakterade funktioner och uppgifter från tjänsteleverantören och överföra dem till alternativa leverantörer eller tillbaka till institutet eller betalningsinstitutet, eller vidta andra åtgärder som säkerställer att den kritiska eller viktiga funktionen eller affärsverksamheten tillhandahålls kontinuerligt på ett kontrollerat och tillräckligt testat sätt, med hänsyn till de svårigheter som kan

[37] Institut, i enlighet med kraven i artikel 85.2 i direktiv 2013/36/EU och kapitel VI i EBA:s riktlinjer för intern styrning, och betalningsinstitut bör ha lämpliga affärskontinuitetsplaner inrättade när det gäller utkontraktering av kritiska eller viktiga funktioner.

uppkomma på grund av var uppgifterna finns, och med de åtgärder vidtagna som behövs för att säkerställa affärskontinuitet under övergångsfasen.

108. När instituten och betalningsinstituten tar fram exitstrategier bör de

a. definiera målsättningarna i exitstrategin,

b. utföra en verksamhetsanalys som står i proportion till risken för de processer, tjänster eller verksamheter som har utkontrakterats, i syfte att identifiera vilka mänskliga och finansiella resurser som krävs för att genomföra exitplanen och hur lång tid detta skulle ta,

c. tilldela roller, ansvarsområden och tillräckliga resurser för hantering av exitplaner och överföring av verksamheter,

d. definiera framgångskriterier för överföring av utkontrakterade funktioner och uppgifter,

e. definiera de indikatorer som ska användas för att övervaka utkontrakteringslösningarna (såsom beskrivs under avsnitt 14), inklusive indikatorer baserade på oacceptabla tjänstenivåer som bör utlösa utträde ur utkontrakteringen.

Kapitel V – Riktlinjer för utkontraktering riktade till behöriga myndigheter

109. När lämpliga metoder fastställs för att övervaka att institut och betalningsinstitut efterlever villkoren för första auktorisation, bör de behöriga myndigheterna eftersträva att identifiera om utkontrakteringslösningar medför en väsentlig förändring av villkoren och skyldigheterna i den första auktorisationen för institut och betalningsinstitut.

110. De behöriga myndigheterna bör förvissa sig om att de ändamålsenligt kan ha tillsyn över institut och betalningsinstitut, däribland att institut eller betalningsinstitut har säkerställt i sin utkontrakteringslösning att tjänsteleverantörer måste bevilja revisions- och åtkomsträttigheter till den behöriga myndigheten och institutet, i enlighet med avsnitt 13.3.

111. Analysen av institutens utkontrakteringsrisker bör som minst utföras inom översyns- och utvärderingsprocessen eller, när det gäller betalningsinstitut, som en del i andra tillsynsprocesser, däribland särskilda förfrågningar, eller under inspektioner på plats.

112. Utöver den information som dokumenteras i registret, såsom avses i avsnitt 11, kan de behöriga myndigheterna be instituten och betalningsinstituten om ytterligare information, i synnerhet för kritiska eller viktiga utkontrakteringslösningar, såsom

a. den detaljerade riskanalysen,

b. huruvida tjänsteleverantören har en kontinuitetsplan som är lämplig för de tjänster som tillhandahålls till det utkontrakterande institutet eller betalningsinstitutet,

c. exitstrategin som ska användas om utkontrakteringslösningen sägs upp av någondera part och om det blir störningar i tillhandahållandet av tjänsterna,

d. de resurser och åtgärder som finns på plats för att tillräckligt övervaka de utkontrakterade verksamheterna.

113. Utöver den information som krävs enligt avsnitt 11 kan de behöriga myndigheterna kräva att instituten och betalningsinstituten lämnar detaljerad information om varje utkontrakteringslösning, även om den berörda funktionen inte anses vara kritisk eller viktig.

114. De behöriga myndigheterna bör bedöma följande enligt ett riskbaserat arbetssätt:

a. Om instituten och betalningsinstituten på lämpligt sätt övervakar och förvaltar i synnerhet kritiska eller viktiga utkontrakteringslösningar.

b. Om instituten och betalningsinstituten har tillräckliga resurser inrättade för att övervaka och förvalta utkontrakteringslösningar.

c. Om instituten och betalningsinstituten identifierar och hanterar alla relevanta risker.

d. Om instituten och betalningsinstituten identifierar, bedömer och på lämpligt sätt hanterar intressekonflikter gällande utkontrakteringslösningar, t.ex. i händelse av utkontraktering inom en grupp eller utkontraktering inom samma institutionella skyddssystem.

115. De behöriga myndigheterna bör säkerställa att institut och betalningsinstitut i EU/EES inte fungerar som ett ”tomt skal”, däribland i situationer där institut använder rygg mot rygg-transaktioner eller transaktioner inom gruppen för att överföra en del av marknadsrisken och kreditrisken till en enhet utanför EU/EES, och bör säkerställa att de har lämpliga styrnings- och riskhanteringsarrangemang inrättade för att identifiera och hantera sina risker.

116. I sin bedömning bör de behöriga myndigheterna ta hänsyn till alla risker, i synnerhet[38]

a. de operativa risker[39] som utkontrakteringslösningen medför,

b. ryktesrisker,

[38] För institut som är underställda direktiv 2013/36/EU, se även EBA:s riktlinjer om ÖUP: https://eba.europa.eu/regulation-and-policy/supervisory-review-and-evaluation-srep-and-pillar-2

[39] Se även EBA:s riktlinjer om IKT-riskbedömning: https://eba.europa.eu/documents/10180/1954038/Guidelines+on+ICT+Risk+Assessment+under+SREP+%28EBA-GL-2017-05%29_SV.pdf/32eff4f9-7607-4b39-b128-02b0030e2ea8

c. ingripanderisken som kan kräva att institutet löser ut en tjänsteleverantör, när det gäller väsentliga institut,

d. koncentrationsrisker inom institutet, däribland på konsoliderad basis, till följd av flera utkontrakteringslösningar med en enda tjänsteleverantör eller nära förbundna tjänsteleverantörer eller flera utkontrakteringslösningar inom samma affärsområde,

e. koncentrationsrisker på sektornivå, t.ex. när många institut eller betalningsinstitut använder sig av en enda tjänsteleverantör eller en liten grupp av tjänsteleverantörer,

f. i hur hög grad det utkontrakterande institutet eller betalningsinstitutet kontrollerar tjänsteleverantören eller har möjlighet att påverka dess handlingar, den riskminskning som kan bli följden av en högre kontrollnivå och om tjänsteleverantören ingår i den konsoliderade tillsynen av gruppen,

g. intressekonflikter mellan institutet och tjänsteleverantören.

117. När koncentrationsrisker identifieras, bör de behöriga myndigheterna övervaka utvecklingen av sådana risker och bedöma både hur de potentiellt kan påverka andra institut och betalningsinstitut och finansmarknadens stabilitet; de behöriga myndigheterna bör när så är lämpligt informera resolutionsmyndigheten om nya potentiellt kritiska funktioner[40] som har identifierats under denna bedömning.

118. När det konstateras orosmoment som leder till slutsatsen att ett institut eller betalningsinstitut inte längre har stabila styrformer inrättade eller inte efterlever regleringskrav bör de behöriga myndigheterna vidta lämpliga åtgärder, vilka kan innefatta att begränsa de utkontrakterade funktionernas omfattning eller kräva utträde ur en eller flera utkontrakteringslösningar. I synnerhet, med hänsyn till institutets eller betalningsinstitutets behov av att arbeta på kontinuerlig basis, skulle upphävda kontrakt kunna krävas om tillsynen och verkställigheten av regleringskrav inte kan säkerställas genom andra åtgärder.

119. De behöriga myndigheterna bör förvissa sig om att de kan utföra ändamålsenlig tillsyn, i synnerhet när instituten och betalningsinstituten utkontrakterar kritiska eller viktiga funktioner som utförs utanför EU/EES.

[40] Såsom definieras i artikel 2.1.35 i direktivet om inrättande av en ram för återhämtning och resolution av kreditinstitut och värdepappersföretag .